## PCT

## WORLD INTELLECTUAL PROPERTY ORGANIZATION International Bureau



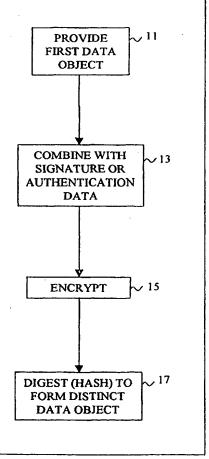
## INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification <sup>7</sup> :		11) International Publication Number: WO 00/1336
H04L 9/32	A1	43) International Publication Date: 9 March 2000 (09.03.00
(21) International Application Number: PCT/US (22) International Filing Date: 27 August 1999 (		(AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, I
(30) Priority Data: 09/144,043 31 August 1998 (31.08.98)  (71)(72) Applicant and Inventor: BORGERS, Frede [US/US]; 105 Mill Valley, Colleyville, TX 76034  (74) Agent: PERDUE, Mark, D.; Zisman Law Firm, 200 sance Place, 714 Jackson, Dallas, TX 75202 (US).	(US). ) Renai	Published  With international search report.  Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

#### (54) Title: METHOD OF AUTHENTICATING OR "DIGITALLY SIGNING" DIGITAL DATA OBJECTS

#### (57) Abstract

A data object, such as a document, is combined or associated with signature or authentication data, such as a time-stamp or signature. Both the data object and the signature data are encrypted. Finally, a distinct data object is generated (digested or hashed) from the encrypted data object and signature data, the distinct data object has characteristics determined by the data object and the signature data. The data object may be hashed or digested prior to being combined with the signature data.



# TO FIGURE OF THE SECOND PROPERTY OF THE PROPER

## 图04077897563、图1661333、1207730。3

O and the control of source of appending or objects. Anomy particularly, and provide the control of the control

## ER BOTOMING AD BOWN COMBON SOLDER FOR COMPRISON

The solution of the solution o

The MAROO BUILDING AND IN THE CHARLES INDONE TO BUILDING YOU BEEN AND AND LIGHT

		ક મુંદ્રક	HSB	FOR THE PURPOSES O	OF INF	ORMATION ONLY	orus ar	W.
		Codes used to identify Sta	ates part	y to the PCT on the front p	ages of	pamphlets publishing inter	national	applications under the PCT
	AL	Albania (139,550)	ĖŚ	Spain G C C Spain	LS	Lesotho	SI *	Slovenia
	AM AT	Armenia Austria	FI	Finland	LT	Lithuania	SK	Slovakia
	AU	Australia	FR	France Gabon	LU	Luxembourg  Latvia 10 10 10 10 10 10 10 10 10 10 10 10 10	SN	Senegal
	AZ	Azerbaijan	GB	United Kingdom	MC	Monaco		
	BA	Bosnia and Herzegovina	GE	Georgia			TD	Chad
	BB	Barbados (a) 19 15 2	GH ::	Ghana ( 2007)	MG:	Republic of Moldova Madagascar	TG STÈ	Talibistan
	BE	Belgium	GN	Guinea	MK	The former Yugoslav	TM	Turkmenistan
	BF	Burkina Faso	GR	Greece		Republic of Macedonia	TR	Turkey
	BG (	Bulgaria Benin	IE U	Hungary Toldand	ML.	Mali Mongolia		Trinidad and Tobago Ukraine
	BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
	BY	Belarus	IS	Iceland Italy	MW	Malawi		
		Canada 1977 17	IT	Italy 2 7	MX	Malawi Mexico	UZ .	Uzbekistan
		Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
		Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
	CH	Switzerland Côte d'Ivoire	KG	Kyrgyzstan	NO .	Norway 1999 1999 1999 1999 1999 1999 1999 19	z <b>z</b> w.o.e	Zimbabwe
		Cameroon	KP					
			KD.	Republic of Korea	PL PT	Poland		
-	CU	Cuba Cuba Billia Bil	ΚZ	Republic of Korea Kazakstan	Ŕď.	Portugal Romania (1970)	1911, N. 11	
		Czech Republic	LC	Saint Lucia	RU	Russian Federation	•	
		Germany	LI	Liechtenstein	SD	Sudan		
	DK	Denmark	LK	Sri Lanka	SE	Sweden		
1	EE	Estonia	LR	Liberia	SG	Singapore		
				Ŧ.				

WO 00/13368 PCT/US99/18824

# METHOD OF AUTHENTICATING OR "DIGITALLY SIGNING" DIGITAL DATA OBJECTS

## TECHNICAL FIELD OF THE INVENTION

The present invention relates in general to providing authentication of digital data, such as document or other data files or objects. More particularly, the present invention relates to methods of securely appending or otherwise incorporating a digital signature or indicia of authenticity into a data object.

## BACKGROUND OF THE INVENTION AND BACKGROUND ART

There have been several prior attempts to digitally "sign," "notarize," or otherwise authenticate a digital data object such as a text document. Generally speaking, one drawback to the storage of, for instance, digital document files, is that it can be difficult to establish whether the version retrieved or transmitted is the identical document originally stored or created. A "digital signature" or "notary" is a common nomenclature for an attempt to provide indicia of authenticity of the digital data.

One such method is found in U.S. Patent Number 5,022,080, June 4, 1991, to Durst et al., which discloses a method of digitally notarizing a document comprising the steps of hashing the document, transmitting the digest (or result of the hash) to a trusted third party, where the digest is combined with a time-stamp, and then encrypting the combination to produce a "digitally notarized" document. All that is required to authenticate the document is the key to the encryption technique. Thus, simply by "breaking the code" the authenticity indicia or the underlying data object can be altered

or tampered with.

1803

Sept Sept at the contract T + 3年 各种的规键

Other solutions complicate this basic scheme to render it more difficult to break the code successfully. For instance, U.S. Patent Number 5,373,561, December 13, 1994 to Haber et al., periodically re-encrypts the signature data to take advantage of everincreasing computational power and advances in encryption, which also render the authentic document more susceptible to alteration, decryption, or tampering as time passes. However, if the user neglects to update? the encryption, the advantage is lost. A need exists, therefore, for a method of digitally authenticating a data object that is not susceptible to future tampering, yet is sufficiently simple as to be implemented in a practical and efficient manner. The treatment of the second one of the contract of the second of t

or the constant property is acquested using the achievage engagements and the a a producer in a discreta movement professor de la move besking beginne besking en la estada estada estada de the first temperature and the property of the The parties of the property assessment to be defined as well to describe medical contract of the original of the a trido es. s.

reductival have an education of the data have a vigorial and girll and

while a religious order may and in each A CARD CONTROL MOTHER EMPTOR CONTROL CONTROL CONTROL TO THE TOTAL CONT of earth with realist, ed. so therefore I make from a trate a cold being a take Charles a record griller roog laar leb is als is bearrafted a roog clarks a room of the later of the com-

建氯铁矿 高级性 神经 化二烷二

## DISCLOSURE OF THE INVENTION

It is a general object of the present invention to provide a method of providing a data object that can ve verified or authenticated reliably, with minimal risk of tampering.

This and other objects of the present invention are achieved by associating or combining a data object, such as a document file, with signature or authentication data, such as a time-stamp or signature. Both the data object and the signature data are encrypted. Finally, a distinct data object is generated or digested from the combination of encrypted data object and signature data, the distinct data object has characteristics determined by the data object and the signature data.

According to the preferred embodiment of the present invention, the generation of the distinct data object is achieved using a hashing algorithm, such as SHA-1.

According to the preferred embodiment of the present invention, the signature or authentication data is provided by a trusted third party. The data object transmitted to the third party may be a digest or hash of the data object to preserve the confidentiality of the data object.

According to the preferred embodiment of the present invention, the encryption step is achieved by a symmetric encryption algorithm.

According to the preferred embodiment of the present invention, the authenticity of the original data object is confirmed by reproducing the distinct data object by identically encrypting a data object identical to the original, generating another distinct data object, and comparing the second and first distinct data objects for identity.

-- 5. --

## BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a high-level flow chart depicting the steps of the method according to the preferred embodiment of the present invention, and more particularly the steps of proving a data object with authentication of signature data.

Figure 2 is a block diagram schematically depicting a portion of the method of Figure 1 according to the preferred embodiment of the present invention.

Figure 3 is a high-level flow chart illustrating the steps of the method according to the preferred embodiment of the present invention, and more particularly of the steps of authenticating a data object provided with authentication data.

Figure 4 is a block diagram schematically depicting a portion of the method of Figure 3 according to the preferred embodiment of the present invention.

the fraction of the best fixer, relied well non-the complete the guingment with the and the state of their state for a substitute of the other which is the experience of the state and the following for the Albert management as with a consequence clayed Crostings of the guilling 19, 19, 6, 19. 4. Agrill 19, 593 of The supported of the Proposition miller aus an Demisia du Maria de Maria this is the total Contest to a soon that a strong toward the sense of the same Survey for group being book of a 14 to 1, to the real for the beginn we are suggested to the Cartest of the first substitute of the substitution and the substitution of the su which distribution is no state given a mojecular in the strong of

ele ili eleti. İriz iniylə əlskerib ine nelimiziməs eli (21 ezend 22 ezend and the situation does its encar-profit estate conventional to the relation source-key may make but

## MODE(S) FOR CARRYING OUT THE INVENTION

Referring now to the Figures, and specifically to Figure 1, a high-level flow-chart depicts the basic steps of a portion of the method according to the present invention.

First, at block 11, a first data object or item is provided by a user or customer of the method. The data object or item could be a document, drawing, image file, or any item or segment of data that the user desires to provide with the ability to be authenticated or become everified in the future of uping details not a word level-field in a foreign.

authentication data. The signature or authentication may include the time of creation of the data object, the name of the author of the object, predetermined characters indicating the origin of the object, or virtually any other data the user desires to serve as evidence of authenticity of the underlying data object. According to the preferred embodiment of the present invention, the authentication data is a "time stamp" that comprises, for instance, the time and date from the "Atomic Clock" maintained by the United States Naval Observatory (e.g., 22:13.02; 4 April 1998). The signature or authentication data is appended, concatenated, or otherwise conventionally combined or associated with the data object. As discussed in greater detail with reference to Figure 2, the time stamp or other signature or authentication data is provided by a trusted third party, perhaps the vendor of the method, who also keeps meticulous records of the method used to combine or associate the data object with signature or authentication data.

Next, at block 15, the combination of the data object and signature or authentication data is encrypted using conventional symmetric secret-key, asymmetric

#### WO 00/13368

150 80 8 8 3 3 7 1

1 1 1 12

public-key techniques or other combining techniques which use a key known only to the trusted third party. The encryption technique could be as simple as appending or concatenating a selected, random text or character string to the data object. For maximum security, it is preferable that the trusted third-party employ secret-key techniques and maintain a record of the encryption technique along with any secret-keys, for future use in authentication of the data object. The preferred encryption method or algorithm is object to a recipient pancy to permit the recipient party to later cordinate

Finally, at block 17, the encrypted data object is digested or hashed using a hash routine to generate a distinct data object. A hash routine generates a data string that is characteristic of the underlying data object that is subjected to the hash routine. The preferred hashing algorithm is SHA-1. There are several hashing routines or algorithms, such as SHA-1, that are suitable for use in the method according to the present invention. All of these hashing routines or algorithms share the following characteristics:

- the underlying data object cannot be reproduced from the hashed data string (it is a one-way of irreversible process); a saltonation
- the routine produces a data string of fixed length; and
- the routine will not yield the same data string for two different data objects. Hashing is sometimes referred to as a method of encryption, but this is inaccurate: the very essence of encryption is that it can be decrypted on the process reversed. Hashing, by its very nature, is not reversible. According to the preferred embodiment of the present invention, the hashing of digesting step may comprise application of a single hashing algorithm or routine to the encrypted data object and signature data.

STURY BOX

. . .

Alternatively, the hashing step may comprise multiple applications of the same or

The result of the hashing step is a distinct data object that has characteristics of both the underlying data object and the signature or authentication data. The distinct data object may be appended to or separate from the underlying data object. The distinct data object and the signature or authentication data is transmitted, along with the original data object to a recipient party to permit the recipient party to later confirm the authenticity of the original data object and/or the combination of the data object and the signature or authentication data is transmitted.

performing the steps of the method according to the present invention. According to the preferred embodiment of the present invention, the encryption and hashing steps are performed on the user's computer 19 which may be a personal computer, a client/server workstation, terminal for a mainframe or minicomputer or the like. The signature or authentication data is provided by a trusted third party 21, who also provides the encryption and hashing algorithms and keeps a record of the encryption or combining techniques and any secret keys for use in future authentication. Alternatively, the encryption and hashing algorithms are resident on and maintained by user's system 19.

According to one embodiment of the invention, the original data object is hashed and then sent to the trusted third party 21 to preserve the confidentiality of the original data object. In this embodiment, the trusted third party performs the encryption and hashing or digesting steps and returns the resulting distinct data object and authentication

data to user 19 to associate with or combine with the original data object.

Communication between user 19 and trusted third party 21 is accomplished in a number of ways: through modem line, T1 line, frame relay link, or cable modem, or http protocol (each with appropriate security). Trusted third party 21 maintains records of any encryption keys, the encryption technique and hashing algorithm(s) for future use by the party that later performs authentication of the document.

Figure 3 is a high-level flow chart depicting the steps of the authentication portion of the method according to the present invention. To authenticate the data object, an original copy, block 31, of the data object, identical to the first, is combined with signature or authentication data, at block 33. The original copy of the data object and signature or authentication data can be provided by the originator, or can be kept by the trusted third party along with the encryption and/or hashing algorithms. After the copy of the original data object is combined with the authentication or signature data, the combinations is encrypted in an identical fashion to the original, at block 35. At block 37, the resulting encrypted data object is then hashed or digested identically to the first, and the resulting distinct data object compared with the original data object (the result of block 17 in Figure 1) and the two are compared for identity. If the two are identical, the than by mind to in the characters in the 其一,使其建立、扩充效力或抗发、治疗病、研究 underlying data object (or the copy) is thus verified or authenticated. If not identical, the data object or copy is not authenticated and cannot be trusted (i.e., the copy or document purporting to be original has been altered and is not identical to the first or the authentication data has been altered).

Figure 4 is a block diagram depicting elements and relationships between entities

performing the steps of the authentication portion of the method according to the present invention. According to the preferred embodiment of the present invention, the authentication steps are performed by a trusted party, perhaps the vendor of the method as the recipient party 25 using information provided by the trusted third party, the originator or user; or a combination of the two. The distinct data objects are input to a comparator or a computer algorithm operable to compare data for identity. The output of the comparator verifies the authenticity (or lack thereof).

According to the preferred embodiment of the present invention, the method is was bodish odi so performed using software resident on the document or data object originator's computer. The encryption and digesting occurs on the trusted third party's computer with the input and results being communicated to and from the trusted third party as described above. The recipient of the "authenticated" data object can request verification through the trusted third party; depending upon which of the parties maintains the requisite encryption technique, hashing algorithm, combination method, and any encryption keys. i ili bilar ili i ei eitolisaadiror

et 1. j. j.

 $\mathcal{T} \sim \mathbb{N}^2$ 

La fefet int gerriet in ing.

The method according to the present invention provides an improved method of a talka haring color pendieser och digitally signing or otherwise authenticating digital data objects. Because the hashing or digesting step is one-way or irreversible, the encrypted portion of the "signature" is not susceptible to unauthorized decryption, even by marked advances in computational undarlying direction to the choice in the power. Because of this advantage, the trusted third party or vendor must keep scrupulous records of the encryption or combining techniques, hashing methods and encryption keys 5 F 250 3 E C FRE 1997 of a surryman employed in providing the signature or authentication data. The win new sell make what notine the

The invention has been described with reference to preferred embodiments thereof. 经国际通过证据的 医阿拉克斯氏征

#### WO 00/13368

It is thus not limited, but is susceptible to variation and modification without departing from the scope and spirit of the invention, which is defined by the claims, which follow.

e com single edicie object out algoriment that

- come ment the description and the expense section of

- come ment centre of the deposition from the completed cata object one significance of the

the medical centre types that my characteristics described dipositions are composited.

in arthodological and the chiral factors computating the state of the second se

on general growing that it with the state of 
The community of the best of the property of the patterned of the patterned of the community of the patterned of the community of the communit

A second of the 
i van er 10 km, 2009 er 1802 er 1802 er 1802 er 1802 er 1802 er 1802 er 1804 er 1804 er 1802 er 1802 er 1802 e I van er 10 km, 2009 er 1802 e

s i albers skie klace pidnog to dishrik usperiledi. Grigerung ar pis pe funcife slagici i i se e per ke data en typkere i elepte

## Superior (CLAIMS) of the following March Shill power of this Joseph Rose and the

1. A method of securely associating signature data with other data, the method comprising the steps of:

associating a data object with signature data;

encrypting both the data object and the signature data; and

generating a distinct data object from the encrypted data object and signature data, the distinct data object having characteristics determined by the data object and the signature data.

- 2. The method according to claim 1 further comprising the step of:
  delivering the distinct data object and signature data to a recipient party.
- 3. The method according to claim 2, further comprising the step of: validating the distinct data object and signature data combination by:

associating a second data object, identical to the first, with the signature data;

encrypting the second data object and the signature data using an encryption method identical to that employed in encrypting the first data object and the signature data;

generating a second distinct data object from the encrypted second data object and the signature data using an method identical to that employed in generating the distinct data object; and

comparing the distinct and second distinct data objects for identity.

- 4. The method according to claim 1, wherein the signature data is provided by a trusted party.
- 5. The method according to claim 1, wherein the encrypting step is performed using a symmetric data encryption technique.

17 97

6. The method according to claim 1, wherein the step of generating the distinct data one in the color by the control of the object is performed using a hash routine.

7. A method of providing a time-stamp for a data object comprising the steps of: generating a distinct value for the data object; associating signature data with the distinct value to produce a signed data object; Perchasing the signed data object; and seems and a seems and a seems and a

generating a second distinct value from the encrypted signed data object, the second distinct data object having characteristics of the encrypted signed data object. principles a second distinct value from the encrypted interest in the encryp-

- 8. The method according to claim 7 further comprising the step of: delivering the second distinct data object and signature data to a recipient party. regrame at the beginning of the Steeling of the Archete and the con-
- 9. The method according to claim 8, further comprising the step of: validating the second distinct data object and signature data combination by: generating a third distinct value, identical to the distinct value; associating a second signature data, identical to the first, with the third distinct value to produce a second signed data object; and

encrypting the second signed data object using an encryption method identical to that employed in encrypting the first signed data object;

generating a fourth distinct value from the encrypted second signed data object using method identical to that employed in generating the second distinct value and an inter-The restriction of the state of

comparing the fourth distinct value and second distinct value for identity. estre est est est eine e control follogen fan 'e dev emplie Crisio est gritegian a

10. The method according to claim 7, wherein the signature data is provided by a trusted Di bis e parti. Les a gelares pièrmes mesém ils quelo el que con e estamentes de

<sup>11</sup> The method according to claim 7, wherein the encrypting step is performed using a symmetric data encryption technique.

PCT/US99/1882

is performed using a hash routine.

(A) The method according to claim 7, wherein the step of generating the distinct value is performed using a hash routine.

(A) The method according to claim 7, wherein the step of generating the distinct value is performed using a hash routine.

generating a distinct value for the data object by performing a hash routine on the data object;

associating a time-stamp with the distinct value to produce a time-stamped data object; the produce a time-stamped data confect; the produce a gain and a state of the produce a gain and the produce as time-stamped data.

generating a second distinct value from the encrypted time-stamped data object by performing a hash routine on the encrypted time-stamped data object.

14. The method according to claim 13 further comprising the step of:

delivering the second distinct data object and time-stamp to a recipient party.

From the containing of how many a stell administrations of manifest has

ra de la cogue a valoridado de regionama do proprio como lo brigada en configir do

15. The method according to claim 13, further comprising the step of:

validating the second distinct data object and time-stamp combination by:

generating a third distinct value, identical to the distinct value;

associating a identical time-stamp with the third distinct value to produce
a second time-stamped data object

encryption method; the second time-stamped data object using the identical encryption method; the particular to the feedback application of the identical

generating a forth distinct value from the encrypted second time-stamped data object; and the second time-stamped with the second time-stamped data object; and the second time-second ti

comparing the fourth distinct value and second distinct value for identity.

16. The method according to claim 13, wherein the time stamp is provided by a trusted party.

All to the site of a ment of hereoth finish a wikeoxabo take the in-

a grand bonned ag a gold pritogram, on near id n. S. nolde of years, we bodd for A. E.

-.: .

17. The method according to claim 13, wherein the encrypting step is performed using

a symmetric data encryption technique.



is un 1/4 and leasing the an early in the array of

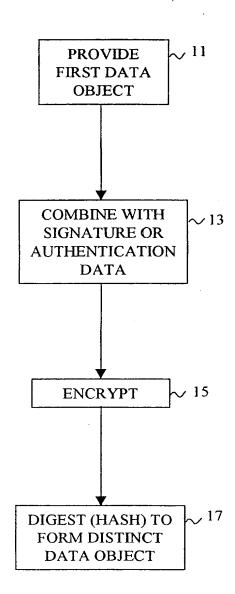


FIG. 1

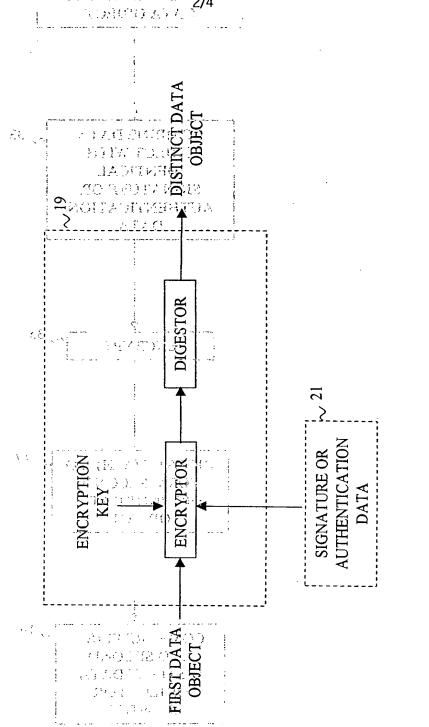


FIG. 2

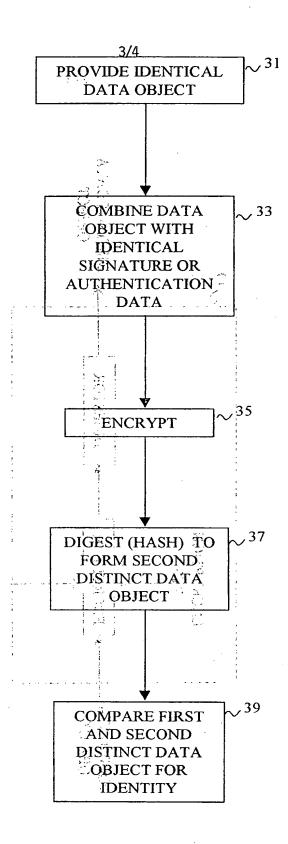
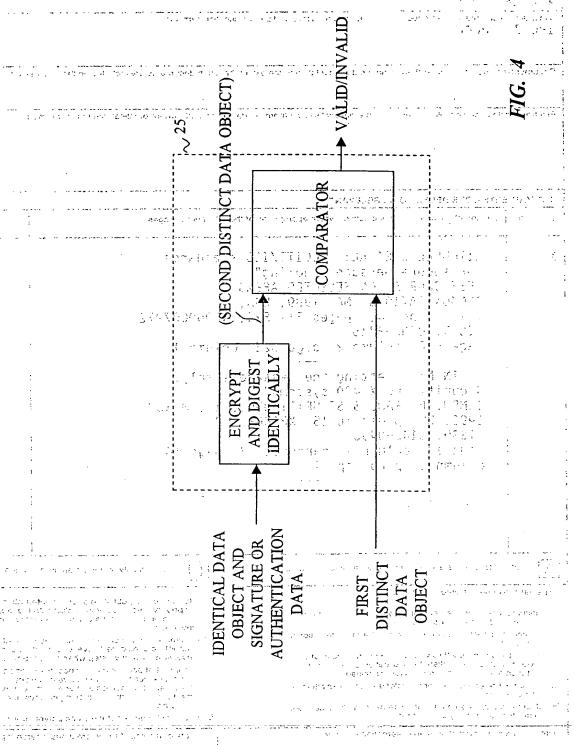


FIG. 3



ON THE

goet haddlassed to

e de estados de el como de el com

. .

5.32.3

## INTERNATIONAL SEARCH REPORT

Inter anal Application No PCT/US 99/18824

7 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1		1 7 7 7 7 7 7 7	
A. CLASS	H04L9/32		
According	to International Patent Classification (IPC) or to both national classifi	cation and IPC	
<del> </del>	SEARCHED		
IPC 7	locumentation searched (classification system followed by classifical H04L	tion symbols)	
	Page 1	such documents are included in the fields searched  ise and, where practical, search terms used)  evant passages  Allevant to claim No.  andards  1-17  000007972  umn 1  afely:  1-17  N, MARCH  8	
Documenta	ation searched other than minimum documentation to the extent that	such documents are included in the fields se	arched
(3	등 등 등 등 등 등 등 등 등 등 등 등 등 등 등 등 등 등 등		
Electronic	data base consulted during the international search (name of data).	ase and, where practical, search terms used	
İ	<u></u> 5	· 18	
	And the second of the second o	L . Z.,	
C. DOCUM	ENTS CONSIDERED TO BE RELEVANT		
Category	Citation of document, with indication, where appropriate, of the re	levant passages	Relevant to claim No.
Х	MITCHELL C ET AL: CCITT/ISD st	andards	1-17
	for secure message handling" [ ] IEEE JOURNAL ON SELECTED AREAS TI	N.	
	COMMUNICATIONS, MAY 1989, USA,		
	vol. 7, no. 4, pages 517-524, X	P000007972	
	ISSN: 0733-8716 page 520, column 2 -page 522, co	lump 1	
	:		
Х	SWAIN N: "Getting the message s	afely.	1-17
	Security and X.400 systems" COMPUTER FRAUD & SECURITY BULLET	IN MARCH	•
	1992, UK, pages 10-15, XP0008629	48	
	ISSN: 0142-0496 page 13. column 1. paragraph 3 -	200 14	
	column 1, paragraph 1	page 14.	
		,	
		-/	
		·	
X Fun	her documents are listed in the continuation of box C	Patent family members are listed in	annex.
Special ca	itegories of cited documents	T" later document published after the intern	national films data
"A" docume	ent defining the general state of the art which is not lered to be of particular relevance	<ul> <li>or priority date and not in conflict with the</li> </ul>	ne application but
	document but published on or after the international	invention	
"L" docume	nate  int which may throw doubts on priority claim(s) or is cited to establish the publication date of another	cannot be considered novel or cannot be involve an inventive step when the doci	e considered to ument is taken alone
citatio	n or other special reason (as specified) ent referring to an oral disclosure, use exhibition or	cannot be considered to involve an inve	intive step when the
other i		ments, such combination being obvious	to a person skilled
later th	nan the priority date claimed	,	
Date of the	actual completion of the international search	Date of mailing of the international sear	ch report
1	7 December 1999	21/01/2000	
Name and r	nailing address of the ISA European Patent Office. P.B. 5818 Patentlaan 2 NL + 2280 HV Rijswijk	Authorized officer	
	Tel. (+31-70) 340-2040. Tx. 31 651 epo nl. Fax: (+31-70) 340-3016	Zucka, G	

1

# INTERNATIONAL SEARCH REPORT

Inter anal Application No

PCT/US 99/18824

,	* . %	<u></u>	PC1/US 99	2/18824
		ation) DOCUMENTS CONSIDERED TO BE RELEVANT		5 D
	Category	Citation of document, with indication where appropriate of the relevant passages		Relevant to staim No
` :	*		1975	~ 20
	□ <b>X</b> - J ] - ] 	US 5 022 080 A (DURST ROBERT T ET AL) 4 June 1991 (1991-06-04)		1-17
		cited in the application column 3,0 line 54		(a2.))
	<b>X</b>	US 5 373 561 A (HABER STUART A ET AL) 13 December 1994 (1994-12-13) cited in the application column 2.44 ne 38 -column 6. line 44		1-17
	X	US 5 638 446 A (RUBIN AVIEL D) 0 0 0 10 June 1997 (1997-06-10) column 3, line 49 -column 6, line 20	To take	1-17
				,
				. 1
				·
			,	
	ĺ			
				·
				,
				1
				,
				:
L			J	

		nfor	NATIONAL SEARCH REPORT mation on patent family members	Einter anal Appli	
2.35	<del>^</del>			PCT/US 99/	
	ätent document d in search repor	t.	Publication PAVE 137 SE Patent fain date	nily (12 miles) 2 miles) (2  Publication :	
US	.5022080	. A	04-06-1991 CA 204		01-12-1992
· .··;	; 			6898 A 🥛 🐰	09-12-1994
US	5373561	Α	13-12-1994 <u>3 nad</u> AU, 25 67( - AU 567)	7,77,73,73,73,73,73,73,73,73,73,73,73,73	04-07-1996 19-07-1994
V [ - ]	<b>!</b>		. A FE A TRAITE CAGA 4215	1590 A.C.	07-07-1994 11-10-1995
	· · +		1. JPs , 1850 1. JPs , 1850 1. Jan 2011 . 3 no. 44	5421 A mad a.	07-07-1994
US	5638446	A	10-06-1997g HRIVANONEGRY &	ask 255 2 18	
	!		7.1777 nph 1107 tu 49 - konitera 6 - 11ne 20	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	<del>,</del>
					· •
	:				
					•
	•				:
					,
					•
					:
					;
	1				:
	1				
	:				
	•				
					:
	·				# * * *
	:				!
	:				; ;
					:
	•				
	i				
		•		•	

٠. :

notes of some notes of the some

TO BE A SULL OF A CONSCIOUS SALES OF MEDICAL PROPERTY.	approximately and the control of the	CALEXS :
FOR ENVIRONMENT COMMENT OF THE STATE OF THE	- 1 1 a	Z. A. (12.8)
en volument in region of the Province of the region of the property of the province of the pro	1000 1000 1000 1000 1000 1000 1000 100	and the control of th
Longit Control to the appropriate of the control to	Commission (1997) (1997	est mar Andulegg († 1. – 11s. 11. A 20s. (12 IVA) 11. G. M. Nath Ween, 2. Ast
The state of the s	The second secon	•

A TO DATO MENGLISH TRUBER OF BUILDING TO STREET OF STANDING OF STA

so the property of the propert



#### WORLD INTELLECTUAL PROPERTY ORGANIZATION International Bureau



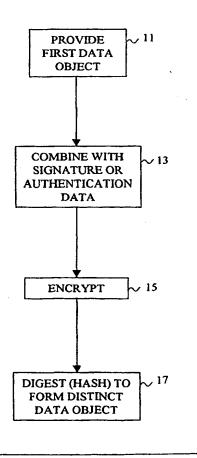
## INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7: WO 00/13368 (11) International Publication Number: **A1** H04L 9/32 (43) International Publication Date: 9 March 2000 (09.03.00) PCT/US99/18824 (81) Designated States: CA. IL. IN, JP. KR, MX, SG, European (21) International Application Number: patent (AT. BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, (22) International Filing Date: 27 August 1999 (27.08.99) IT, LU, MC, NL, PT, SE). Published (30) Priority Data: 09/144,043 31 August 1998 (31.08.98) US With international search report. Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of (71)(72) Applicant and Inventor: BORGERS, Frederick, [US/US]; 105 Mill Valley, Colleyville, TX 76034 (US). (74) Agent: PERDUE, Mark, D.; Zisman Law Firm, 200 Renaissance Place, 714 Jackson, Dallas, TX 75202 (US).

#### (54) Title: METHOD OF AUTHENTICATING OR "DIGITALLY SIGNING" DIGITAL DATA OBJECTS

#### (57) Abstract

A data object, such as a document, is combined or associated with signature or authentication data, such as a time-stamp or signature. Both the data object and the signature data are encrypted. Finally, a distinct data object is generated (digested or hashed) from the encrypted data object and signature data, the distinct data object has characteristics determined by the data object and the signature data. The data object may be hashed or digested prior to being combined with the signature data.



صارب و المعدد مسوم ما والأول 143 " and the second 11 21 1 a 於 医结肠和 食物區 156 ्रम्पूर्वे अपूर्वन होते हैं। जिस्सी असे हुम राज्य के विकास करें SON HERE THOUGH Some fragilian in a resident 1965年1月1日 - 1962年 福田市中央社会 (公司) FOLEROLINASTY the of Law of the Entertwood State マルテルのg whitesthe / classes not (代数) TORK OF BURNESS OF BETT AND STAGE IS NOT SELECTED BY A POST OFF and the control of th A COMBRIDAD VOVIDAL ELEGISTO AUX DIBITADA ACA CIUNA COLONA (CA ASAG PERFURNOU PO OPILIABO EPE NON PERFURING CELIONA CONTRARA CRIPTED IN CORP. PARKE SOCIETY MANAGEMENT OF CONTROL OF CORP. en de la companya de la companya de la companya de la companya de la companya de la companya de la companya de and the second of the second of the second re sale policy to more than (74) Vertical Mer on Ennio (50) United Bird (ECC) (1.80 e/95 eC. (1.10 ft in negethics most a Buren ber Sa popular Analysis ing the bud to a first the second (इस्मे नज्य कर्मा रूपा है। To the work of the second of t untplumenting to the life of t ್ ಕ್ರಾರ್ಡ್ ಕ್ರಾರ್ಡ್ ಕ್ರಾರ್ಡ್ ಕ್ರಾರ್ಡ್ ಕ್ರಾರ್ಡ್ 💆 Complete and some property of the complete and the complete and comple 1.45

FOR THE PURPOSES OF INFORMATION ONLY

man ship

性性 医水性细胞 活

4. . . . .

THE PROPERTY WAS ARREST OF PROPERTY.

THOM spages got was been able with a con-

nd horse stony, non-Abres for the confirmation of the confirmation

ELECTION OF THE PROPERTY OF THE PARTY OF THE

LYMAGROOD - A POST - 15

AL	Albania	ES	Spain	: LS	Lesotho	SI	Slovenia	
4M	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia	
AT	Austria	FR	France	LU	Luxembourg	SN		
AU.	Australia	GA	Gabon	LV	Latvia	SZ	Senegal Swaziland	
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad	
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo	
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan	
BE	Belgium	GN	Guinea	MK	The former Yugoslav	TM	Turkmenistan	
BF	Burkina Faso	GR	Greece	1	Republic of Macedonia	TR	Turkey	
BG	Bulgaria	HU	Hungary	ML	Mali	TT		
BJ	Benin	ΙE	Ireland	MN	Mongolia	UA	Trinidad and Tol Ukraine	oago
3R	Brazil	IL	Israel	; MR	Mauritania	UG		
BY	Belarus	IS	Iceland	MW	Malawi	US	Uganda	
CA	Canada	IT	Italy	MX	Mexico	UZ	United States of	America
CF	Central African Republic	JP	Japan	NE	Niger	VN	Uzbekistan	
CC	Congo	KE	Kenya	NL	Netherlands	YU	Viet Nam	ė
CH	Switzerland	KG	Kyrgyzstan	i NO	Norway		Yugoslavia	F
CI -	Côte d'Ivoire	KP	Democratic People's	NZ	New Zealand	ZW	Zimbabwe	<u>i</u>
M	Cameroon		Republic of Korea	PL	Poland			¢1
CN	China	KR T	Republic of Korea	PT				
CU	Cubaco ទីស្គារ មករយៈភូមិរាម៉ា	KZ	Republic of Korea Kazakstan	RO	Pomenia		or native contrastic	13.7
Z	Czech Republic	· · · · · · · · · · · · · · · · · · ·	Saint Lucia: 19 19 19 18 2	ាន វិធីស្រាំ 🤄	Romania Russian Federation	525 Jahre	tatik Milabir	
E	Germany		Liechtenstein 300 mil. 23 m	e i oʻsb ⇒	Suden Carlon	5 5 7	e germanika	-
K	Denmark	LK `	Sri Lanka		Sweden	7 t		• •
EΕ	Estonia	LR	Liberia		Singapore			×'

which are a section of the section